INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 5)
Available online at: www.ijariit.com

A comprehensive survey on IoT networking

Anirban Mukherjee
anirban.mukherjee2016@vitstudent.ac.in
Vellore Institute of Technology, Vellore, Tamil Nadu

Aditya Singh
aditya.singh2016a@vitstudent.ac.in
Vellore Institute of Technology, Vellore, Tamil Nadu

ABSTRACT

This paper rummages into the stirring world of the Internet of Things (IoT), which in recent years has soared in popularity and practical applications. Today it connects diverse devices of various forms from all across the planet into a sophisticated yet unified system. IoT is revolutionizing modern lives with all its features and implementations across many multiple domains like healthcare, broadcasting, safety, etc. However, with the rise of IoT, it has also raised apprehensions about the networks which need to evolve as they are the pivots of IoT devices. IoT devices can be prone to network attacks due to a lack of proper protocols for managing the IoT devices, jeopardizing crucial data. This survey thus aims to summarize the working of IoT across networks, looking into its working and components, its current challenges and limitations, the security and privacy concerns plus its countermeasures.

Keywords—*ARP, BIOS, ETSI, IoT, DNSNA, MAC, MIRM, UpnP*

1. INTRODUCTION

As we progress further into the modern internet era, the expansion of internet and communication technologies have had such an explosive impact that our lives are now completely dependent on IoT and its various real-life applications. People can chat, work, maintain their schedule, shop, and watch TV in the services provided by IoT. So, we look into the various applications of IoT devices and how it affects human beings. We also delve into the multiple challenges that prevent the complete utilization of the IoT devices which can help our lives for the better. Therefore, in this paper we delve into the latest implementations of IoT devices [1] across diverse domains, looking into its working, various applications as well as its limitations. We find that networking plays an extremely crucial role in implementing a smooth implementation of IoT services over multiple domains. Thus, we analyse the various networking techniques, optimizations, limitations and the latest work being done on it to provide even better services.

The paper also looks into the various security features and flaws currently present in IoT devices due to ill-defined protocols or the advent of new features and how do we tackle them successfully. This will bring positive changes to the future society, possibly changing our way of life for the better. Good business models and possible areas of research can make it happen sooner than we think.

To do this we look into various implementations of IoT applications and the approaches used that make the IoT devices work, improve its performance, introduce new features and solve its limitations. We look into its various advantages and disadvantages, possible future work and the various factors that influence it.

2. APPLICATIONS

2.1. In-band full-duplex wireless communications and networking for IoT devices

This paper delves into full-duplex wireless and its applications in IoT systems as compared to half-duplex systems used earlier. It also summarizes the performance of the full-duplex with experiments comparing it while achieving the in-band full-duplex in wireless communications. In doing so, it compares it with crucial parameters like the Throughput performance and the Packet Reception Ratio of full-duplex to that of half-duplex in software-assisted and well-defined radio platform. In this paper, the authors have suggested methods in order to cancel self-interference and then highlighted the advantages of in-band full-duplex over the presently used half-duplex wireless communications. This includes the overall Physical layer throughput improvement and also solving hidden terminal problems in the MAC layer. Thus full-duplex wireless overshadows half-duplex wireless on both the throughput and performance. The authors observe that as soon as the traffic bit rate increases, full-duplex wireless immediately shows its advantages with better throughput and Packet Reception Ratio (PRR). This is due to the busy tone that is present in the network, which is useful to prevent collisions exacerbates in half-duplex wireless as soon as the traffic becomes more cumbersome. Currently, there are still challenges present in order to achieve in-band full-duplex wireless so that it can be used in the real world

but unfortunately no method currently can cancel self-interference from 20 to 90 dBm except the Stanford design, which is limited to Wi-Fi protocol 802.11ac with 80 MHz bandwidth in the 2.4 GHz range and 20 dBm average TX power, thus presenting multiple limitations.

The authors observe that further research is indeed needed to design better duplex commodity radios, which possess better chip-size and supports more protocols and bandwidth in an energy-efficient manner. Also, new MAC and routing protocols are the need of the hour to enable full-duplex networking. If successful, it would revolutionize data transfer in wireless networks such as Wi-Fi networks and potentially in 5G and above services with much better efficiency and speed. [2]

2.2 A reliable IoT system for Personal Healthcare Devices

Healthcare applications in IoT have been skyrocketing in demand because they allow remote monitoring of patients. Keeping that in mind, this paper proposes a oneM2M-based IoT system for Personal Healthcare Devices. For using a Personal Healthcare Device as an Application Dedicated Node in this proposed system, it needs a protocol conversion between ISO/IEEE 11073 protocol messages and oneM2M protocol messages which take place in the gateways located between the Personal Healthcare Devices and the Ph.D. management server. It is done to use a Ph.D. as an Application Dedicated Node in the proposed system. In the authors' experiments to test their system, the results show that the following protocol conversion performs quite effectively and efficiently; not causing the system to suffer severe issues performance-wise, even if the number of Application Dedicated Node is more extensive than usual.

The modules for the working of the system include CMDH (Communication Management/Delivery Handling) which provides data delivery service in the network. It decides the time and the method regarding how the data is to be delivered. DMG (Device Management) which handles device management. NSSE (Network Service Exposure/Service Execution and Triggering) which controls the communication related to the base network and provides network access via an MCN reference point. Resource Handler which controls the resource tree that stores information regarding all objects dealt by the system. Message Handler and Protocol Converter which examine the received messages, in order to perform all the necessary operations in the message. It also converts ISO/IEEE 11073 messages into oneM2M messages and vice versa.

The framework first receives the message from the Ph.D., and after that, the Network Manager module located in the gateway sends the message to the Message Handler and Protocol Converter module so as to examine the message and convert the necessary protocols. The Message Handler and Protocol Converter module settles on the protocol type to be utilized so as to transmit the conveyed message. In the case where ISO/IEEE 11073 convention is to be executed, the module takes the required data from the message to build the oneM2M Primitive Request message(s), which are sent to the Resource Manager module. Other data in the conveyed message is stored in the gateway, to be utilized when the related Response message is sent back to the Ph.D. The Resource Manager module is in charge of dealing with the resource tree that stores the vital data for oneM2M messages. After accepting the oneM2M Primitive message(s) from the Message Handler and Protocol Converter module, the Resource Manager module executes the essential activities as indicated by the oneM2M message. At that point, the oneM2M Primitive Response messages are developed to convey the activity results/status to the Message Handler and Protocol Converter module. Upon accepting the oneM2M Primitive Response message(s) from the Resource Manager module, the Message Handler and Protocol Converter module changes over the message(s) into the comparing ISO/IEEE 11073 Response message, so as to convey them to the Network Manager module. Finally, the Network Manager module sends the ISO/IEEE 11073 Response message to the Ph.D.

However, its real-life testing is yet to be performed. Therefore, it is performances when applied to actual medical scenarios are yet to be seen, but it has shown considerable promise and can potentially change the healthcare system for the better. [3]

2.3. SpEED-IoT: Spectrum aware energy-efficient routing for device-to-device IoT communication

This paper proposes a multi-hop multi-channel routing scheme called "SpEED-IoT" for D2D communication in IoT mesh network. Here, the authors have used spectrum sensors that gain relevant information regarding Spatio-temporal spectrum usage. Their scheme finds the best route, best available channels at each hop along the route, and the optimal transmission power required for each hop. They have tested their scheme's performance concerning factors like connectivity and reachability between all the IoT devices with different spectrum conditions, data optimization, effectiveness in licensed incumbent protection, and degree of fairness while assigning routes to multiple interfering devices. The transmission power control proposed in SpEED-IoT uses a selective flooding technique to limit the overhead of route request forwarding and thereby preserves precious energy resources of the IoT devices. The model also utilizes an evolutionary game theory technique played on the side of the interfering end-to-end D2D routes. They demonstrate that an equilibrium exists where the sensors can maximize overall network performance and achieves fairness, unlike ad-hoc or greedy based route assignments.

The working model consists of:

A primary network that is a centralized network consisting of licensed base stations as transmitters and a collection of receivers associated with base stations, e.g., cell towers. The primary networks are mutually exclusive from the secondary IoT devices. These primary networks possess prioritized access to the licensed spectrum. We then have Environmental sensing capacity where we assume that the sensors comprising the ESC are deployed in the region of interest which can be chosen randomly or be carefully planned. Each sensor possesses a transmission range of r_s and the secondary IoT devices within the range are under the view of the sensor. It then consists of a Spectrum map. The spectrum map/REM, which is created periodically by the ESC is a 3-D representation showing spectrum utilization. The models/techniques used for creating these maps allow secondary networks to compute/predict the spectrum usage at random locations. As mentioned earlier, the secondary IoT devices are the ones who try to access the channels not utilized by the primary network. It is assumed that secondary IoT devices are used notwithstanding of primary and sensor

locations. These IoT devices are cognitive radio disabled and therefore possess no spectrum sensing capability. The idea is that whenever the source and destination devices are not under the same sensor, flood the route request in the neighboring domains. That being said, present energy constraints in IoT devices do not permit the appropriate usage of DSR or AODV inspired flooding. Therefore, SpEED-IoT uses a selective flooding approach.

This proposed model allows for licensed incumbent protection, IoT device energy preservation, effective end-to-end data rate optimization, and fast convergence and fair route assignment among interfering D2D communications. That being said, this research was only conducted on a simulation-based testbed, a practical implementation may prove to be inefficient. [4]

2.4. 5G-enabled devices and smart-spaces in social-IoT

On the topic of 5G technologies, this literature discusses 5G technology. It looks into the context - awareness in smart systems and space discovery paradigms such as online versus offline, the femtocell usage and the energy aspects which are to be considered, and about the ongoing social IoT applications. They elaborate on the most significant components in smartphone usage and also categorize the existing tracking apps in this area. They talk about smartphone and mobile application testing, and issues faced during it like device fragmentation, OS fragmentation, and simulation environments. They then proceed to talk about the usage of femtocells, which is a cellular network base station that connects standard mobile devices to a mobile operator's network using residential cable broadband connections, optical fiber or wireless last-mile technologies which is a vital component of all modern wireless telecommunication systems. The authors talk about energy aspects and discuss open issues in modern-day data usage, the most important of them being the privacy of users while trying to discover user patterns, which while helps a lot in optimizing the users' experience, is a threat to the users and the service providers. This survey covers much ground on 5G technology and brings to light the topic of femtocells. Femtocells access the Internet instead of using the usual cellular operator network. This results in customers having better service, improved coverage, and signal strength since they are closer to the base station. Using femtocells leads to a longer battery lifespan due to its close proximity to the femtocell. While the survey shows the great marvels of the femtocell networks, it also shows that there are a variety of issues on the energy efficiency of femtocell networks which need to be investigated in the future, like energy metrics and energy consumption models regarding not only femtocells but also femtocell and macro-cell heterogeneous networks and the effect of interference problem on femtocell energy consumption. [5]

2.5. A framework for DNS naming services for Internet-of-Things devices

As IoT devices keep increasing in number, it is getting more and more difficult for users to control and monitor their devices. To resolve this lingering issue, the authors propose a new naming framework for "Domain Name System Name Autoconfiguration" (DNSNA) for IoT devices using IPv4 and IPv6 networks. The goal of the "DNSNA" is to provide DNS naming services to IoT devices under IPv4 and IPv6 networks so that users can easily recognize them. DNSNA tackles the aforementioned growing challenge effectively and enables the users to monitor or remote-control the IoT devices in their local network or across the Internet. DNSNA utilizes a unicast protocol for DNS name resolution rather than multicast and consists of the standard protocols, such as Neighbour Discovery, Node Information Query, and Dynamic Host Configuration Protocol. In the proposed DNSNA, the users can easily register and control the DNS names of IoT devices. DNSNA checks the aliveness of a device's service with the help of periodic message polling. According to the experimental results, it can be concluded that mDNS, which is the current naming scheme, cannot manage the services of IoT devices efficiently and correctly. So, DNSNA can be considered to be the better protocol in IoT environments rather than mDNS. However, the fact that the time interval of Node Information (NI) Query of DNSNA, which is used for IoT device discovery and service discovery, has been getting meagerer and the packet volume hs been getting larger may pose a problem in some cases during its implementation. [6]

2.6. FitCNN: A cloud-assisted and low-cost framework for updating CNNs on IoT devices

One of the most prominent implementations of IoT devices in our daily lives is done using Cloud Computing. Keeping that in mind, in this paper, the authors have observed that Convolutional Neural Network (CNN) is one of the most critical topics in modern-day computing as it has successfully achieved near impeccable accuracy in image classification and recognition tasks. CNNs are generally deployed in the cloud to handle data collected from the IoT devices, such as smartphones and other unmanned systems. That is why enormous data transmission overhead and privacy issues have made CNNs vital to be used directly on the device side. However, the trained model deployed on mobile devices cannot handle the unknown data and objects in new environments as effectively, potentially causing low accuracy and poor user experience. This makes it crucial to retrain models that suit the needs of the modern-day IoT services. That being said, due to high computing costs and memory usage, training a CNN on IoT devices with limited hardware resources is impractical. To solve this issue, the authors note that the usage of cloud services in order to assist mobile devices train a deep neural network can effectively tackle this challenge. For that purpose, this paper proposes a cloud-assisted CNN framework, called "FitCNN", possessing incremental learning as well as low data transmission, for reducing the overhead of updating CNNs deployed on the existing devices, which may lead to slow speeds and many unsatisfied customers. FitCNN uses strategies called: the juicer and distiller to upload only the essential data and use light weights, making it easier for the devices to process the data. The experiments show that the Distiller strategy reduces 39.4% overhead of the uploading transmission on the datasets, and the Juicer strategy can reduce up to 60% of data transmission costs for updating the old models present on devices. It means that there is no longer a need for a paramount internet connection, it has much better privacy and security, and there is no significant overhead during transportation of data back and forth to the IoT devices. However, in the off chance if relevant data cannot be found, it will be hard to get practical results as the data then would have to be trained with idealistic data which are hard to unearth and it would need proper hardware for the IoT devices to be able to handle the deployment. [7]

2.7. Design and implementation of a novel service management framework for IoT devices in the cloud

In this paper, the authors have designed a cloud framework called "SMFIC" (Service Management Framework for IoT devices in Cloud) for handling real-time data generated from multiple IoT devices and social media sites and as well as for processing the non-

real time data for scientific computation and storage. Here the application layer is also considered as the data source layer. IoT devices generate an enormous amount of real-time and batch data on multiple environments and are sent to the cloud for analysis. The non-IoT sub - layer generates requests to process those stored data. The sub-layer consists of various components or users such as the individual researcher, smart healthcare centers, government agencies, and business entities. The abstraction of the various modules under the application layer is in the form of the IoT sub-layer and non- IoT sublayer. This allows the Cloud Service Provider (CSP) to generalize the service for all IoT based devices and to expand their capabilities without having to create diverse frameworks for every type of IoT service present immensely benefitting the Cloud Consumer. However, the division of labor in the form of various modules like the Application handling layer and request preprocessor make the handling of some form of IoT services cumbersome and involving many overheads as not all services require such a sophisticated service framework. This framework also involves rebuilding a lot of existing CSP platforms from the ground up. [8]

2.8. A lightweight machine learning-based authentication framework for smart IoT devices

As we can see, although our lives have vastly improved enhanced by IoT devices, IoT applications still do contain challenges in securing the networks and the data during transit. Existing security solutions, such as everyday password-based two-factor authentication and the traditional biometric-based authentications, can be vulnerable since threats can significantly affect the reliability and efficiency of the entire system. Thus the authors realize that there is a need for a highly secure authentication mechanism in the currently existing networks. Hence, they propose "Cancellable Biometric System" (CBS). "CBS" is a biometric template protection scheme that works on repeated distortions/transformations at the feature/signal level. So the authors propose a framework for a cloud-based lightweight cancellable biometric authentication system that can be used with high accuracy and minimum overhead without compromising the security. The storage of feature level transformation of the biometric template is stored in centralized servers. The templates possess the one-way property, and multiple transformed templates can be generated from one source. This can lead to instant and smooth delivery of cloud services, even for small and medium-sized businesses, since it has minimal setup costs and time. [9]

2.9. How to footprint, report and remotely secure compromised IoT devices

The paper delves into the process of securing our IoT devices to prevent any unwanted malpractice. It does so by the mapping of IP addresses by using external footprinting techniques – e.g., retrieving an autonomous system number/country using "WHOIS", abuse email contact(s), and geolocating the address. The paper classifies nodes by using active footprinting techniques – e.g., TCP port scan, and operating system (OS) family detection, etc. The paper proposes a model that creates reports which notify the information gathered by the previous footprinting process, to the shareholders such as law enforcement, or third-party blocking services. The securing process is the one that involves intrusion techniques used in order to gain remote access to a vulnerable or compromised IoT device, but to prevent further unauthorized access from TELNET which includes changing device passwords, terminating suspicious processes, terminating the Telnet daemon, and so on. The paper then discusses a prototype model Fooresec which relies on an external process such as a honeypot, an IDS/IPS, a firewall, etc. to obtain public IP addresses that are to be footprinted, reported and secured. It is an exhaustive process that aims to control the aspects of the footprinting and to secure the nodes. The proposed system is quite flexible with regards to what is to be done after the data discovery process. The securing process is also efficient and robust. As the model is still up-and-coming, the author notes that these systems rely on various external services as well as applications. Therefore, it has a lot of dependencies and overheads. The host system requires a significant overhaul in terms of current hardware to implement Foorsec technology in existing nodes, which makes it a little challenging for large scale implementation. It can also get quite rigid from time to time and can accept little to no change. [10]

2.10. Towards occupant activity driven smart buildings via Wi-Fi-enabled IoT devices and deep learning

The paper proposes DeepHare: A deep learning-based human activity recognition system that can automatically identify the everyday activities using only basic commodity Wi-Fi-enabled IoT devices. In order to achieve this, the authors have designed an Open Wrt-based IoT platform that collects Channel State Information (CSI) measurements from the commercial IoT devices. After this, they designed a deep learning framework called "Autoencoder Long-term Recurrent Convolutional Network" (AE-LRCN). Using this model, the CSI (Channel State Information) can analyze and show human activity in a non-intrusive manner as the body movements made during various activities would interfere with the signal propagation paths and give rise to a high variation of CSI. Experiments show that the model can successfully identify typical human behavior and activities with 97.6% recognition accuracy by leveraging only two commodity Wi-Fi routers with zero human intervention. For now, the machine learning framework still needs tedious feature engineering, and there are security concerns in implementing DeepHare in real-time applications regarding the storage of data that are being looked upon for broader implementation in the future. [11]

2.11. Risk-based automated assessment and testing for the cybersecurity certification and labeling of IoT devices

Nowadays, security is a problem in the implementation of large-scale IoT. Being able to certify and communicate with the devices is crucial. In this paper, they provide a security certification methodology designed for the large-scale communication between IoT devices. This methodology provides transparency to the IoT at security level as it provides a label which is the main result of the certification. The certification approach represented an instantiation of the Risk-based Security Assessment and Testing methodologies presented by ETSI and has been built on top of different technologies and approaches for security on IoT landscape. They considered the automated testing approach from the "ARMOUR" project, in order to face the IoT challenges related to dynamism and scalability. A labeling activity had been integrated within the Communicate and Consult process. The proposed certification approach is intended to certify a certain TOE. A TOE is defined as a set of software, firmware or hardware possibly accompanied by guidance. The proposed method includes the automation of the whole process by means of technologies such as MBT, CertifyIt, and TITAN to design, generate and execute the security tests, in such a way that the recertification process can be made in an easy way. The proposed method is intended to serve as a corner-stone to define a more consistent and standardized approach. [12]

2.12. The art of mapping IoT devices in networks

In this paper, the authors propose a method to map an IoT device in a network. IoT device is proliferating but many have a weak security control. They have used several existing scanning techniques to identify IoT devices on IP range. UPnP scans (Universal Plug and Play) networking protocols allow devices on the network to discover each other and indicate network seamless for seamless communication. NetBIOS scans are functionality that allows applications on remote machines to communicate within a LAN. The characteristic of NetBIOS names that can be exploited to discover IoT devices is that these names often indicate the type of device on an IP address. MAC-to-vendor resolution maps IP addresses to physical addresses in the LAN. OS identification Nmap network mapper is an industry-standard tool-of-choice for network engineers and administrators. TCP and UDP ports can provide an insight into the type of device functioning on an IP address. The process begins by entering IP address ranges to be scanned. Hardware addresses are resolved to vendor names since the first three octets in a MAC address belonging to specific vendors and can be used to identify manufacturers. An unknown label indicates that it is not a major vendor so it is a candidate for IoT devices. Devices with UPnP enabled revealed their device's descriptions and other details via XML files during their scanning. ARP scans are used to discover devices active in the local network. The Nmap OS identification database is used to recognize the operating system of the remote host. Formal asset registration and management process track every device brought into the network before it is allowed to communicate and is the best defence against rogue IoT devices. The current techniques fall short when trying to discover IoT by themselves. A conjunction of these techniques can assist administrators in recognizing an IoT device on a network. regular scanning of the list of registered IoT devices will help in quickly assessing against vulnerabilities and commence patching. [13]

2.13. The potential risk of IoT device supporting IR remote control

In this paper, the authors check attacks on a smart TV set-top box, using malicious IR hardware module (MIRM). They list countermeasures for prevention and enhance security of IR remote control and eliminate such covert channels. In the attack model, a MIRM is made and implanted into a keyboard with a supply chain attack or malicious maintenance. Sensitive data, such as credit card numbers, passwords are sent to the MIRM via TTL-level signals by the malware. The MIRM converts the TTL-level signals to IR remote control commands and sends them to a nearby TV box. The data is obtained by accessing the log file on the website. The countermeasures include countermeasures for IR remote control and countermeasures against covert channels. There are two methods in countermeasures for IR remote control. The first method is to avoid to use IR remote control. The second method is to give a prompt tone for every received command. The types of countermeasures against covert channels are threefold: design countermeasures, procedural countermeasures, and technical countermeasures. [14]

2.14. Towards automatic fingerprinting of IoT devices in the cyberspace

In this paper, the authors propose an efficient approach to generate fingerprints of IoT devices. They observed that device manufacturers had different network system implementations on their products. They explored feature spaces of IoT devices in three network layers, including the network-layer, transport-layer, and application layer. Using the feature of network protocols, they generate IoT fingerprints based on neural network algorithm. They implement the prototype system and conduct real experiments to validate the performance of devices' fingerprints. Results show that their classification can generate device labels with a 94A% precision and 95% recall. They use these device fingerprints to discover 15.3 million network-connected devices and analyse their distribution characteristics in cyberspace. They define the device fingerprint in three-level granularity: the device type, vendor and product. Device types and vendors are kept fixed during a relative period. They utilize a two-stage approach to provide a label to a packet based on the collected data. The neural network generates device fingerprints that would provide class label of the IoT device. In the neural network, each neuron extracts the finger-grained features from three layers, including network-layer, transport-layer, and application-layer. The algorithm is checked on a dataset created from Amazon using Scrapy framework to scrape web pages from commercial websites of device vendors. The precision achieved was 94.7% at the device type level, 93.3% at the vendor level and 91.45 at the product level. Their technique can detect the device label and provide a comprehensive analysis of the composition of those compromised vendors. [15]

2.15. Temporal traffic smoothing for IoT traffic in mobile networks

In this paper, the authors propose a communication timing control for temporal and spatial traffic offloading that works for moving IoT devices in cellular networks. By their method, part of the excess traffic is moved to off-peak times and neighbouring cells. The system consists of a system server and IoT devices. the system server is connected to each IoT device via an application-level network. The system server and IoT devices communicate using an application layer protocol such as Http. the procedure starts when the system server detects a congested base station. The system server then sends instructing messages to IoT devices connected to the base station. The instructing message indicates the time until when the IoT devices should delay their requests. the IoT device calculates the amount of the utility that it will obtain if it follows the instructions. Then it decides whether to delay the request or not by calculating a response probability from the utility and comparing it with what it will obtain if it does not follow the instructions. The evaluation conducted a simulation study to verify whether their method effectively smoothes traffic of IoT applications in mobile networks. they examined their method through a simulation using realistic IoT traffic models an actual mobility dataset of vehicles. The results proved that their method outperforms the no-control case and two other control methods in terms of reducing peak traffic and meeting latency requirements. [16]

3. CHALLENGES AND OPEN ISSUES IN HANDLING THE PROBLEM

There still remain numerous issues and hurdles in IoT as it is still a growing sector. As of now, there are still technological difficulties regarding interoperability and integration [17] of various features into IoT. The advent of IoT applications and smart gadgets having enhanced inter-device communication will lead to smart systems possessing high degrees of intelligence. Its autonomy will enable fast deployment of diverse IoT implementations over complex domains and will create newer services, leading to numerous new territories regarding software and hardware. Therefore, alongside the Internet and Communication-related technologies, there should be a focus on designing hardware and software having a small size, low cost, yet sufficient functionality. As IoT is a growing sector,

there are hurdles regarding future issues and problems as the topics are diverse and growing. Standards play an influential role in IoT as well. A standard is essential to allow all actors to access and use equally. The advancement and coordination of standards and protocols will promote the efficient growth of IoT infrastructures, applications, services, and devices. Also compared with traditional networks, security, as well as privacy issues regarding IoT, are much more prominent with severe consequences, making the strengthening of networking protocols a significant aspect concerning modern-day IoT applications.

4. CONCLUSION

IoT technologies have an immense impact on our modern lives. Today, we can confidently say IoT will successfully replace many existing methods and techniques of doing tasks for the better. In the near future, it will interconnect people as well as devices across the world at unison. The performance of people's ventures and numerous communication technologies will transcend expectations with the help of IoT devices. This unusual nature of IoT, which is in a state of flux makes it a fascinating domain to work on, which will significantly improve today's nature of computing and networking. However, the rise of IoT has also created concerns regarding data privacy and security [18] and tackling it has been identified as a vital challenge for IoT. In this survey, we presented the Internet of Things with its various applications, challenges, the vital role of networks in building working IoT models with its development and challenges, and the methods for resolving the challenges regarding IoT, factors that affect the performance of IoT devices as well its future possibilities. We surveyed the security and privacy concerns of IoT as well. In addition, we identified several open concerns related to the security certifications, solutions, and privacy that need to be addressed by the research community to make a secure and trusted platform for the delivery of future Internet of Things. We also discussed applications of IoTs in real life. In the end, we can conclusively say that research on the IoTs will remain a hot topic, and there are still many things yet to be explored and worked upon in IoT.

5. REFERENCES

[1] Bhaddurgatte, R. C., & Kumar, V. (2015). A Review: QoS Architecture and Implementations in IoT Environment. *Research & Reviews: Journal of Engineering and Technology*, 6-12.

[2] Wu, S., Guo, H., Xu, J., Zhu, S., & Wang, H. (2017). In-band full-duplex wireless communications and networking for IoT devices: Progress, challenges, and opportunities. Future Generation Computer Systems.

[3] Woo, M. W., Lee, J., & Park, K. (2018). A reliable IoT system for personal healthcare devices. Future Generation Computer Systems, 78, 626-640.

[4] Debroy, S., Samanta, P., Bashir, A., & Chatterjee, M. (2019). SpEED-IoT: Spectrum aware energy-efficient routing for device-to-device IoT communication. Future Generation Computer Systems, 93, 833-848.

[5] Al-Turjman, F. (2019). 5G-enabled devices and smart-spaces in social-IoT: an overview. Future Generation Computer Systems, 92, 732- 744.

[6] Lee, K., Kim, S., Jeong, J. P., Lee, S., Kim, H., & Park, J. S. (2019). A framework for DNS naming services for Internet-of-Things devices. Future Generation Computer Systems, 92, 617-627.

[7] Liu, D., Yang, C., Li, S., Chen, X., Ren, J., Liu, R., ... & Liang, L. (2019). FitCNN: A cloud-assisted and low-cost framework for updating CNNs on IoT devices. Future Generation Computer Systems, 91, 277-289.

[8] Dehury, C. K., & Sahoo, P. K. (2016). Design and implementation of a novel service management framework for IoT devices in the cloud. Journal of Systems and Software, 119, 149-161.

[9] Punithavathi, P., Geetha, S., Karuppiah, M., Islam, S. H., Hassan, M. M., & Choo, K. K. R. (2019). A Lightweight Machine Learning-based Authentication Framework for Smart IoT Devices. Information Sciences.

[10] Lauria, F. (2017). How to footprint, report and remotely secure compromised IoT devices. Network Security, 2017(12), 10-16.

[11] Zou, H., Zhou, Y., Yang, J., & Spanos, C. J. (2018). Towards occupant activity driven smart buildings via WiFi-enabled IoT devices and deep learning. Energy and Buildings, 177, 12-22

[12] Matheu-García, S. N., Hernández-Ramos, J. L., Skarmeta, A. F., & Baldini, G. (2019). Risk-based automated assessment and testing for the cybersecurity certification and labeling of IoT devices. *Computer Standards & Interfaces*, *62*, 64-83.

[13] Pranshu Bajpai, Aditya K Sood, Richard J Enbody, (2018). The art of mapping IoT devices in networks. *Network Security 2018(4)*:8-15

[14] Zhou, Z., Zhang, W., Li, S., & Yu, N. (2019). The potential risk of IoT devices supporting IR remote control. *Computer Networks*, *148*, 307-317.

[15] Yang, K., Li, Q., & Sun, L. (2019). Towards automatic fingerprinting of IoT devices in the cyberspace. *Computer Networks*, *148*, 318-327.

[16] Yamada, Y., Shinkuma, R., Iwai, T., Onishi, T., Nobukiyo, T., & Satoda, K. (2018). Temporal traffic smoothing for IoT traffic in mobile networks. *Computer Networks*, *146*, 115-124.

[17] Banafa, A. (2017). Three major challenges facing iot. *IEEE IoT Newsletter*.

[18] Gasiorowski-Denis, E. (2016). How the Internet of Things will change our lives. *ISO News*, *5*.

